## REMARKS

Claims 1-15 remain pending.

CLAIM REJECTION UNDER 35 USC §102

At page 2 of this Office Action, claims 8-11 are rejected under 35 U.S.C § 102(e) as being anticipated by U.S. Patent No. 6,584,566 to Hardjono. Applicants submit that claims 8-11 are not anticipated by Hardjono because Hardjono does not disclose all of the elements of Applicants' invention.

Claim 8 recites the step of "from a list of top tier key encryption keys, selecting a top tier key encryption key that does not correspond to a group that includes the compromised node [emphasis added]". Applicants submit that Hardjono does not teach the top tier key encryption key selection step recited in claim 8. At numbered response 4 of this Office Action, it is asserted that "a key encryption key (SGK) is used to encrypt new key information being multicasted to other top-tier servers or sent one at a time". Applicants submit that SGK taught by Hardjono is a key designated for a multicast to a group of key servers (see Col. 6, lines 25-34). "All key servers involved in the common multicast group are a member of a separate multicast instance, called the server multicast group or server group (SG)". Id. In particular, Hardjono teaches that "server control and/or key management information is multicast to the key servers using the server group key [emphasis added]." See Col. 6, lines 50-52. Nothing is disclosed or suggested by Hardjono that the selected SGK does not correspond to a group that includes a compromised node.

In the event of re-keying, Hardjono teaches two methods of notification (see Col. 8, lines 34-56). One method taught by Hardjono uses SGK which is common to all key servers in the group. Clearly, using SGK is contrary to "selecting a top tier key encryption key that does not correspond to a group that includes the compromised node" as recited in claim 8 because no exclusion of a compromised node is made using SGK. Hardjono teaches to multicast SGK to all key servers regardless of the presence of a compromised node related to any key server. An SGK taught by Hardjono is not a top tier key encryption key that does not correspond to a group that includes the compromised node.

The second method taught by Hardjono is using the private server specific KSKs. However, using KSKs also does not exclude compromised nodes. To isolate a leaving member, Hardjono teaches to use a separate and different non-top tier key that has a characteristic to make such key secure from the leaving member. For example, KSK is used in the second method because "members" do not have access to KSK. No top tier key, that does not correspond to a group that includes the compromised node, is selected in accordance with the teaching of Hardjono.

In essence, Hardjono teaches to use a variety of "group" specific keys for distributing a pair of common group keys, namely an initial CGK and a replacement CGK that is swapped out for the initial CGK when re-keying is desired. In contrast with the Applicants' invention, Hardjono takes an entirely different approach to re-keying encryption keys. The keys taught by Hardjono represent a variety of keys used to communicate between and among the key servers and the members (see FIG. 1). DK is used by a key server to communicate with all members in the domain while MK is used for individual communication between the key server and a specific member. SGK is used for communication among all of the key servers while KSK is used for communication between the initiator key server and a specific key server.

Finally, Hardjono does not disclose the step of "encrypting a new traffic encryption key using the top tier key encryption key, to produce an encrypted traffic encryption key [emphasis added]" as recited in claim 8. Although Hardjono teaches that a key server, having a node where a member is leaving, can notify other key servers through the server multicast group using key SGK or using a private key (e.g., KSK:C), nothing is disclosed or suggested by Hardjono that a new traffic encryption key is encrypted using the top tier key encryption key (see Col. 8, lines 45-56). In fact, Hardjono teaches that key servers can notify other key servers through a multicast to such key servers using SGK, regardless of whether a compromised node is associated with such key server. Re-keying does not occur using SGK as taught by Hardjono.

Instead, Hardjono teaches that "each key server without a client membership change distributes the replacement common group key to its multicast members using its domain key" and "the key server(s) with a member leaving distribute the replacement common group key and a new domain key to its remaining members using the member keys" (see Col. 9, lines 1-

42). Hardjono discloses a specific example where a domain-key (e.g., DK:A) is used to encipher the replacement common group key which is then multicast. However, such domain key is not a top tier key encryption key, and any analogy made of the domain key to a top tier key would be in direct conflict with referring to SGK as a top tier key. Hardjono simply does not teach encrypting a new traffic encryption key using the top tier key encryption key but rather teaches to use a replacement common group key.

Applicants' respectfully submit that claim 8 is patentably distinguished from Hardjono because Hardjono does not teach the top tier selecting step nor the encrypting step recited in claim 8. Because of the foregoing discussion regarding the patentability of claim 8 and because claims 9-11 depend from claim 8, Applicants respectfully submit that claims 9-11 are likewise patentably distinguished from Hardjono.

At page 3 of this Office Action, claims 12-15 are rejected under 35 U.S.C § 102(b) as being anticipated by U.S. Patent No. 5,592,552 to Fiat. Applicants submit that Fiat does not disclose all of the elements of Applicants' invention.

Claim 12 recites as an element "a storage device coupled to the encryption device, the storage device being configured to hold a hierarchy of key encryption keys [emphasis added]." Although Fiat discloses a system having n subscriber memories storing a set of keys (see Fiat, claims 17-20), Fiat does not teach or suggest a hierarchy of key encryption keys. Disclosure of a partitioning scheme for a population of subscribers by Fiat (see Col. 12, line 58 – Col. 13, line 10) is in the context of key, or multiple keys, distribution to the subscribers. At best, Fiat teaches that a different number of keys are stored in different subscriber memories based on subscriber population. In one example, Fiat teaches an n-leaf balanced binary tree where the subscribers, the lowest level (see Fiat, FIG. 3) receive log r keys, r being the number of subscribers. Although Fiat discloses privileged sets of subscribers and providing keys respectively corresponding to a set of all possible subscriber subsets within an n-member subscriber population, the nature of the keys (i.e., associated with a hierarchy) is not hinted at by Fiat (see Col. 11, lines 18-65).

Further, although Fiat discloses encryptors, Fiat does not disclose a storage device coupled to the encryption device where the storage device is configured to hold a hierarchy of

key encryption keys as recited in claim 12. Any reference in Fiat to a storage device is to the subscriber memories that may hold various sets of keys corresponding to all possible subscriber subsets. Applicants submit that subscriber memories taught by Fiat is not the storage device recited in claim 12. Fiat does not teach a hierarchy of key encryption keys nor a storage device configured to hold the same. Fiat does not mention any relationship between the encryptors and the subscriber memories.

Applicants' respectfully submit that claim 12 is patentably distinguished from Fiat because Fiat does not teach "a storage device being configured to hold a hierarchy of key encryption keys" as recited in claim 12. Because of the foregoing discussion regarding the patentability of claim 12 and because claims 13-15 depend from claim 12 or an intermediate claim depending therefrom, Applicants respectfully submit that claims 13-15 are likewise patentably distinguished from Fiat.

From the foregoing discussion, Applicants submit that rejection of claims 8-15 under 35 U.S.C § 102(b) has been overcome.

CLAIM REJECTION UNDER 35 USC §103

At page 2 of this Office Action, claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,584,566 to Hardjono as applied to claims 8-11 above, and further in view of U.S. Patent No. 6,684,334 to Srivastava and further in view of U.S. Patent No. 6,195,751 to Caronni et al. Applicants submit that claims 1-7 are not obviated by Hardjono in view of Srivastava and Caronni et al. because none of the cited references, either alone or in combination, disclose all of the elements of Applicants' invention and because there is no motivation to combine Caronni et al. with Hardjono and Srivastave, either alone or in combination.

Claim 1 recites the step of "broadcasting a new traffic encryption key to each of a plurality of top tier groups in a top level tier, wherein the plurality of top tier groups excludes a group that includes the compromised node". As previously set forth hereinabove with regard to the patentability of claims 8-15, Hardjono discloses that the pair of CGKs is initially distributed to all key servers (see Col. 4, lines 63-66), and the initial CGK is subsequently distributed to clients of the key servers that are members (see Col. 5, lines 24-31). In response to re-key

needs, Hardjono discloses that the initiator key server multicasts a new initial and replacement CGK (Col. 8, lines 57-60). Hardjono also discloses that the replacement CGK is distributed to the clients of the key servers that are members (see Col. 5, lines 37-46). However, Hardjono does not teach or suggest distributing the replacement CGK to each of the key servers excluding the key server having the compromised node. In contrast, Hardjono teaches to multicast to all key servers a new initial and replacement CGK. The key server, domains, and members all receive the replacement CGK such that the group including the compromised node is not excluded.

As previously mentioned hereinabove, Hardjono teaches that key servers can notify other key servers through a multicast to such key servers using SGK, regardless of whether a compromised node is associated with such key server. Re-keying does not occur using SGK as taught by Hardjono. Applicants submit that SGK taught by Hardjono cannot be analogized with "a new traffic encryption key" as recited in claim 1 because nothing discloses that SGK changes in any fashion. Instead, Hardjono teaches that a replacement CGK, such as one enciphered using a domain key, is multicast.

Srivastava is cited for disclosing a multiple level multicast group. In particular, Srivastava teaches that a group controller generates a new key for a parent of a leaving node as well as all ancestral nodes until the root node is reached. For example, the group controller encryps a new key of the parent node with the adjacent node/s private key (see Col. 18, lines 49-56). Caronni et al. disclose a system for secure multicast using a first key that is shared with all participant entities and a set of second keys that is shared with a subset of the participant entities. This group key management component stores and maintains the first and second keys in a group key database that is in a non-hierarchical, flat fashion (see Col. 4, lines 41-51). Caronni et al. are cited in this Office Action for disclosing recursive broadcasting. Applicants submit that Caronni et al. do not teach recursive broadcasting as recited in claim 1, and that there is no motivation to combine Caronni et al. with Hardjono or Srivastava.

Claim 1 recites the step of "within the group that includes the compromised node, recursively broadcasting the new traffic encryption key to groups of nodes at a succession of lower tiers". In contrast, Caronni et al. discloses that during exclusion of a participant, an

excluder chooses a new TEK that is encrypted with all KEKs not shared with the participant. The KEKs known to the participant are thrown out, and new KEKs are assigned. This information populates a table which is sent to the participant group. The other participants able to decrypt the new TEK supplements the table with new KEKs which it holds and rebroadcasts the table. This rebroadcasting taught by Caronni et al. has no effect on groups at successively lower tiers. Caronni et al. simply teaches broadcasting an updated table with new KEKs to other participants without any reference to a tier structure. Further, Hardjono does not provide any guidance as to broadcasting the new traffic encryption key to groups of nodes at a succession of lower tiers. Instead Hardjono teaches secure unicast using member keys, not broadcasting to groups of nodes at a succession of lower tiers.

Applicants submit that there is no motivation to combine Carroni et al. with Hardjono or Srivastava because Carroni et al. teach contrary to Hardjono and Srivastava. Carroni et al. teach that a respective participant has a TEK and one or more KEKs and independently chooses a new TEK and assigns new KEKs during re-keying (see Col. 14, lines 55-67). In contrast with Carroni et al., Hardjono teaches that key servers multicast a new pair initial CGK and replacement CGK, and Srivastava teaches that new keys are created from a parent node to the root node including sub-branches hanging off from sub-nodes that fall on the path from the departed node to the root node. Hardjono and Srivastava teach completely different methods of re-keying than Carroni et al.

Furthermore, Applicants submit that the hypothetical combination of Caronni et al. with Hardjono and Srivastava, either alone or in combination, does not result in Applicants' invention. In particular, Caronni et al. teaches the use of a non-hierarchical, flat fashion key organization which implies no tier grouping of keys. Any resulting combination of Caronni et al. with Hardjono and/or Srivastava would include the flat fashion key organization which is completely contrary to the teachings of Hardjono and Srivastava as well as to Applicants' tier group hierarchy. There is nothing in Caronni et al. that suggests that rebroadcasting from one participant to other participants in a participant group may be applied in the sense of rebroadcasting to groups of nodes at a succession of lower tiers. Additionally, Srivastava is silent as to any broadcasting or rebroadcasting of new traffic encryption keys.

Applicants' respectfully submit that claim 1 is patentably distinguished from the cited references, either alone or in combination, because the cited references do not teach nor suggest the steps recited in claim 1. Because of the foregoing discussion regarding the patentability of claim 1 and because claims 2-7 depend from claim 1 or an intermediate claim depending therefrom, Applicants respectfully submit that claims 2-7 are likewise patentably distinguished from the cited references.

From the foregoing discussion, Applicants submit that rejection of claims 1-7 under 35 U.S.C § 103(a) has been overcome.

CONCLUSION

In view of Applicants' amendments and remarks, it is respectfully submitted that the rejections under 35 U.S.C. §102(b) and (e) and §103(a) have been overcome. Accordingly, Applicants respectfully submit that the application, as amended, is now in condition for allowance, and such allowance is therefore earnestly requested. Should the Examiner have any questions or wish to further discuss this application, Applicants request that the Examiner contact the Applicants' attorneys at 480-385-5060.

If for some reason Applicants have not requested a sufficient extension and/or have not paid a sufficient fee for this response and/or for any extension necessary to prevent abandonment on this application, please consider this as a request for an extension for the required time period and/or authorization to charge Deposit Account No. 50-2117 for any fee which may be due.

Respectfully submitted,

INGRASSIA FISHER & LORENZ, P.C.

Dated: July 30, 2004

By: _____

Andrew Y. Pang
Reg. No. 40,114
(480) 385-5060